

**AMENDMENTS TO THE DRAWINGS**

Figures 1, 9, 10, 12, 13, 15 and 16 have been amended to correct the spelling of "terminal". No new matter is added.

Attachments: Annotated Drawing Sheets Showing Changes  
Replacement Drawing Sheets

### REMARKS

Reconsideration and allowance of the subject patent application are respectfully requested.

The drawings have been amended to correct the spelling of "terminal" in Figures 1, 9, 10, 12, 13, 15 and 16.

The specification has been amended to correct minor informalities including those noted on page 3 of the office action.

The claims have been amended to address the informalities noted on page 3 of the office action.

Claims 1-15 were rejected under 35 U.S.C. Section 102(e) as allegedly being "anticipated" by Lai On (U.S. Patent Publication No. 2002/0059531). While not acquiescing in this rejection, claims 1-9, 11-13 and 15 have been amended and claims 10 and 14 have been canceled without prejudice or disclaimer. The discussion below makes reference to the amended claims.

Claim 1 is directed to an authentication system provided with a server system communicably connected to a communication terminal. A first authentication unit receives user-identifying information from the terminal and authentication is carried out based on the user-identifying information. As described by way of example without limitation in the subject patent application, the user-identifying information may be a user ID, a password, a license number, etc. First key information is generated based on the authenticated user-identifying information, and the generated first key information is transmitted to a user of the terminal. As described by way of example without limitation in the subject patent application, the first key information may be an access key. A second authentication unit receives the first key information from the terminal and generates second key information and transmits the second key information to the terminal. As described by way of example without limitation in the subject patent application, the second key information may be a session key. The second key information is transmitted from the terminal to the server and the terminal is allowed to access the data in the server using the second key information for a specified period of time. In the example embodiments, when the access time reaches the specified period of time for the second key information, the user

terminal can obtain additional second key information using the first key information. Thus, when the user needs additional access, only second key information is needed.

Based on the above, in the non-limiting example embodiments, for plural times of access to the data in the server, the user-identifying information is transmitted only once to the server (e.g., in the case of a communication navigation, when the power is turned "on"), thereby reducing the possibility of revealing a user's private information. Additionally, in the server, generating a session key is simpler than generating an access key, and thus the computation load of the server can be reduced as well.

A non-limiting example of the effectiveness of the disclosed embodiments can be better understood by imagining a long drive, for example, from Washington D.C. to Florida along an unknown road. During the drive, the driver may make frequent requests to a communication navigation terminal (e.g., restaurants, sightseeing spots, etc.). In such a case, once the driver enters his/her personal information into the communication navigation terminal for authentication, there is no need to input personal information again as long as, for example, the ignition key is at "ACC" or "ON." Instead the access key, which has been acquired at the beginning, can be used to simply obtain session keys that allow access to the server each time. It is thus very convenient and provides higher security for the driver and reduces the work to be carried out by the server. The higher security comes from the combination of the time limitation for the access and the double-key-use scheme.

In contrast, Lai On provides a "one-authentication system" utilized by a plurality of vendors (multiple partnered vendors: see paragraph [0013]). A detailed flowchart is shown in Figure 3, in which a user session key and a second site's key are used in accessing multiple vendors (steps 301 to 308). That is, in Lai On, when an already-acquired user session key is sent to the server, the user is able to receive the second site's key already registered in the server. Therefore, the user's access to a second vendor can be authenticated.

The use of first key information and second key information in claim 1 is not disclosed or suggested by the use of the user session key and the second site's key in Lai On. In particular, in the claimed system, the first and second key information function as a two-stage authenticating process for accessing data in the server. Moreover, unlike the claimed arrangement, Lai On fails to propose a scheme of providing a specified period of time of access when the second key

information is used (e.g., "second key information entitling the user to repeatedly access to the data in the server system for a specified period of time" in claim 1).

Therefore it is respectfully submitted that claim 1 is not anticipated by Lai On.

Independent claims 4 and 8 include similar features and are likewise not anticipated by Lai On.

New claims 16-20 have been added. Support for the subject matter of claim 16, for example, can be found in the description and accompanying figures for the first embodiment of the subject patent application. Lai On does not disclose the utilization of access and session keys set forth in claim 16 and thus this claim and claims 17-20 that depend therefrom are believed to patentably distinguish over this reference.

The pending claims are believed to be allowable and favorable office action is respectfully requested.

Respectfully submitted,

**NIXON & VANDERHYE P.C.**

By: \_\_\_\_\_



Michael J. Shea  
Reg. No. 34,725

MJS:mjs  
901 North Glebe Road, 11th Floor  
Arlington, VA 22203-1808  
Telephone: (703) 816-4000  
Facsimile: (703) 816-4100